(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－282393

(43)公開日　平成９年(1997)10月31日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	19/00			Ｇ０６Ｆ	15/42	Ｊ
	15/00	３３０			15/00	３３０Ｇ
Ｇ０６Ｋ	17/00			Ｇ０６Ｋ	17/00	Ｌ
Ｈ０４Ｌ	9/32			Ｈ０４Ｌ	9/00	６７３Ｃ
						６７３Ｅ

審査請求　未請求　請求項の数10　ＯＬ　（全 12 頁）

(21)出願番号　特願平8－91117

(22)出願日　平成８年(1996)４月12日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　木戸　邦彦
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　佐野　耕一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

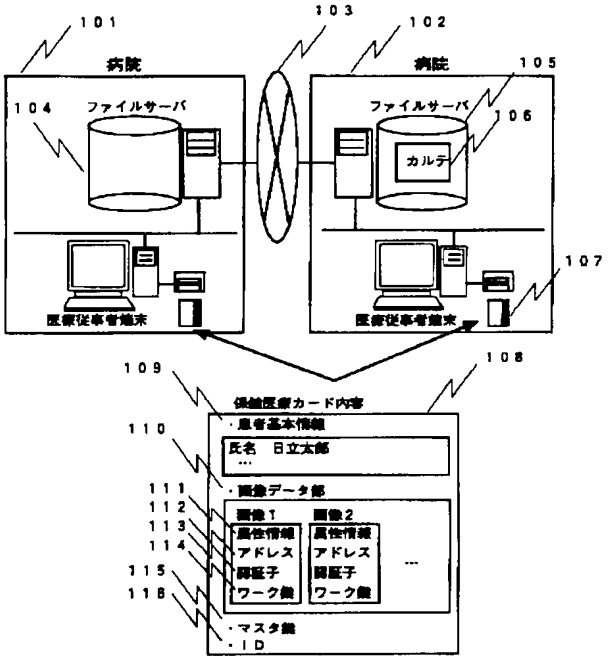
(74)代理人　弁理士　磯村　雅俊

(54)【発明の名称】　保健医療カードとオンラインデータベースの連携方法

(57)【要約】

【課題】画像などの大容量データの蓄積保存を可能にするとともに、従来のオフライン型保健医療カードと同じ安全性を確保する。また、カードを紛失したときにオンラインデータベースから安全にカードの内容を復元する。

【解決手段】マスタ鍵をカードごとに割り振って、ＩＣカードに保存する。患者データは、ワーク鍵で暗号化しデータベースに登録した後、データを保存するデータベースのネットワーク上でのアドレスとデータベース上のデータを特定する識別子（ファイル名）をＩＣカードに保存する。次に、所定のハッシュ関数を利用してデータの認証コードを作成し、これもＩＣカードに保存する。また、データを登録する病院には、ＩＣカードのＩＤとともにデータを暗号化するために使用したワーク鍵をカードのマスタ鍵で暗号化したものや、鍵暗号鍵を記録する。



【特許請求の範囲】
【請求項１】複数の医療機関に分散設置された通信端末装置と、該通信端末装置との間で情報の授受を行う保健医療カードと、該通信端末装置を結合する通信網と、該通信網に接続され、上記複数の医療機関によって共有される複数のデータベースとを有する保健医療カードとオンラインデータベースの連携方法において、
上記保健医療カードには、上記データベースの少なくとも一つに登録されるデータごとに設定され、該データを登録したデータベースを通信網において特定するネットワークアドレス情報と、
該データベース内の当該データの詳細な所在を特定するファイル名情報と、
上記データベースに登録したデータから予め定められた一方向性ハッシュ関数により計算した数値の認証子と、
上記データベースに登録するデータに施す暗号処理に使用したワーク鍵情報とを格納することを特徴とする保健医療カードとオンラインデータベースとの連携方法。
【請求項２】請求項１に記載の保健医療カードとオンラインデータベースの連携方法において、
前記複数のデータベースの少なくとも一つには、当該データが格納されている保健医療カードごとに一意に付与されたＩＤ番号と、
当該データを暗号化するために使用したワーク鍵情報を該カードのマスタ鍵情報で暗号化した情報、あるいは該マスタ鍵情報を暗号化して該ワーク鍵情報を生成するために使用した鍵暗号鍵情報と、
該データベース内の当該データの詳細な所在を特定するファイル名情報とを記録しておくことを特徴とする保健医療カードとオンラインデータベースの連携方法。
【請求項３】請求項１または２に記載の保健医療カードとオンラインデータベースの連携方法において、
データ暗号化のための前記ワーク鍵情報の生成処理、データの暗号化処理、および認証子の生成・検証処理を上記保健医療カード内で行うことなく、全て端末通信装置で行う場合には、
前記複数のデータベースの少なくとも一つには、当該データが格納されている保健医療カードごとに一意に付与されたＩＤ番号と、
当該データを暗号化するために使用したワーク鍵情報を該カードのマスタ鍵情報で暗号化した情報と、
該データベース内の当該データの詳細な所在を特定するファイル名情報と
を記録しておくことを特徴とする保健医療カードとオンラインデータベースの連携方法。
【請求項４】請求項１に記載の保健医療カードとオンラインデータベースの連携方法において、
前記複数のデータベースの少なくとも一つに登録されたデータは、ある医療機関からの検索要求により、当該データが登録されているデータベースを通信網において特定するネットワークアドレス情報と、
該データベース内の当該データの詳細な所在を特定するファイル名情報とに基づいて、該データベースから通信網を介し検索要求を行った医療機関の通信端末装置に転送されることを特徴とする保健医療カードとオンラインデータベースの連携方法。
【請求項５】請求項１または３に記載の保健医療カードとオンラインデータベースの連携方法において、
前記検索要求を行った医療機関は、登録されたデータベースから転送してきた当該データを受け取ると、
当該データに対して、データベース登録時に施され、暗号処理に用いられたワーク鍵情報を予めカードから得ておき、
該ワーク鍵情報を基に復号処理を施すことを特徴とする保健医療カードとオンラインデータベースとの連携方法。
【請求項６】請求項１，３または４に記載の保健医療カードとオンラインデータベースの連携方法において、
前記検索要求を行った医療機関は、請求項４に記載の復号処理を行ったデータに対して、予め定められた一方向性ハッシュ関数により認証子を計算し、
該認証子と保健医療カード登録されている認証子とを比較し、
比較の結果、同一と判定されたときには、上記復号処理を行ったデータは正しいものとして該医療機関のメモリに格納することを特徴とする保健医療カードとオンラインデータベースの連携方法。
【請求項７】複数の医療機関に分散設置された通信端末装置と、該通信端末装置との間で情報の授受を行う保健医療カードと、該通信端末装置を結合する通信網と、該通信網に接続され、上記複数の医療機関によって共有される少なくとも一つのデータベースとを有する保健医療カードとオンラインデータベースの連携方法において、
当該保健医療カードの媒体は、上記データベースと通信網を介して接続し、該データベースの一つに登録する各データごとに、該データベース内の当該データの詳細な所在を特定するファイル名情報を入手して、自媒体内に格納するが、
その際に、該ファイル名情報を該保健医療カードと該データベースとが共有する鍵情報により暗号化して通信することを特徴とする保健医療カードとオンラインデータベースとの連携方法。
【請求項８】請求項７に記載の保健医療カードとオンラインデータベースの連携方法において、
前記保健医療カードと当該データベースとが共有する鍵情報により暗号化して通信する際の暗号処理は、該保健医療カードの内部で行うことを特徴する保健医療カードとオンラインデータベースとの連携方法。
【請求項９】請求項７に記載の保健医療カードとオンラインデータベースの連携方法において、

前記複数の医療機関によって共有される少なくとも一つのデータベースには、保健医療カードごとに一意に付与されたＩＤ番号とともに当該データの詳細な所在を特定するファイル名情報を記録しておき、
上記共有されるデータベースとは異なる各医療機関等のデータベースには、該共有データベースの一つに登録されるデータに施す暗号処理に必要な少なくとも２つの鍵情報のうちの一つとともに、上記保健医療カードごとに一意に付与されたＩＤ番号を記録しておくことを特徴とする保健医療カードとオンラインデータベースとの連携方法。
【請求項１０】請求項９に記載の保健医療カードとオンラインデータベースの連携方法において、
前記共有されるデータベースとは異なる各医療機関等のデータベースには、該共有データベースの一つに登録されるデータに施す暗号処理に使用したワーク鍵情報とともに、上記保健医療カードごとに一意に付与されたＩＤ番号を記録しておくことを特徴とする保健医療カードとオンラインデータベースとの連携方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、保健医療カードシステムをオンラインデータベースと連携させた場合にも、盗聴、改竄等にさらされないように安全性を確保することができる保健医療カードとオンラインデータベースの連携方法に関する。
【０００２】
【従来の技術】従来より、保健医療カードは、患者の病歴、薬歴をＩＣカードに記録しておくことによって、患者の健康状態の変化を経時的に観察することができるため、質の高い診療や医療相談等に役立つ点で注目されていた。保健医療カードのその他の利点としては、異なる病院間にまたがって診察、治療を行っている患者に関して、処方された薬品や実施された検査データが記録されているため、薬品の重複投与や重複検査がさけられることである。また、薬品に関しては、異なる病院で処方された薬品に、薬品相互作用を引き起こす組み合わせがないか否かをチェックすることができるため、薬品相互作用による薬害を防止することが可能である。しかしながら、保健医療カードは、個人の健康状態に関するデータが蓄積されているため、その内容を不特定の第３者に知られると、プライバシー保護の観点から望ましくない。従って、通常は、カードにアクセスするための認証処理を行っている。認証処理としてアクセスチェックを行うためには、カード自体にマイクロプロセッサを埋め込み、そのマイクロプロセッサによりアクセス権のチェックを行うことができるようなＩＣカードが必要となる。
【０００３】
【発明が解決しようとする課題】しかしながら、現在のところ、ＩＣカードの記憶容量は、画像のような大容量データを蓄積保存するには小さ過ぎるため、記録されるデータとしては文字テキストベースの数値データや医師等の所見が主である。同様な理由により、ワードプロセッサ等で記述されたカルテのような非定型的なデータを、ＩＣカードにファイルの形で蓄積することも難しい。そこで、大容量のデータはネットワークにつながれたオンラインデータベースに登録しておき、そのアドレス情報はＩＣカード側で管理して、ＩＣカードとオンラインデータベースと連携させることにより大容量データに対応する手法が考えられる。ただし、単純にオンラインデータベースのアドレスをＩＣカードで管理しただけでは、患者のプライバシーが守れない。このように、ＩＣカードという物理的に安全な媒体に患者情報を記録することによって、患者のプライバシーが守れるのに対して、このＩＣカードをオンライン環境と連携するときには、安全性が崩れてしまうという問題が生じる。オンライン環境における脅威としては、ネットワークにつながれたデータベース上にあるデータが改竄されること、およびネットワーク上あるいはデータベース上での盗聴などが挙げられる。ここで、特に問題になる点は、患者データが登録されるデータベースを管理している正当なユーザが、自分に不都合なデータを改竄することも考慮しなければならないことである。例えば、誤診などで訴訟を起こされた病院が、データを操作する場合などが考えられる。なお、従来のオフライン型の保健医療カードでは、普段は患者がカード自体を所持しているため、上記のようなネットワーク上あるいはデータベース上の不正は不可能である。本発明の目的は、このような課題を解決し、従来のオフライン型保健医療カードと同じ安全性を、オンラインデータベースと連携した保健医療カードシステムに対して実現できるような保健医療カードとオンラインデータベースの連携方法を提供することにある。また、本発明の他の目的は、ＩＣカードを紛失したときにも、オンラインデータベースから安全にそのＩＣカードの内容を復元することができる保健医療カードとオンラインデータベースの連携方法を提供することにある。
【０００４】
【課題を解決するための手段】上記目的を達成するため、本発明による保健医療カードとオンラインデータベースの連携方法では、（ａ）複数の医療機関（図１の１０１，１０２）に分散設置された通信端末装置（図２の２０１）と、該通信端末装置との間で情報の授受を行う保健医療カード（図１の１０７，１０８）と、該通信端末装置を結合する通信網と、該通信網に接続され、上記複数の医療機関によって共有される複数のデータベースとを有する保健医療カードとオンラインデータベースの連携方法において、上記保健医療カードには、上記データベースの少なくとも一つに登録されるデータごとに設定され、該データを登録したデータベースを通信網（図

１の１０３）において特定するネットワークアドレス情報（図１の１１２）と、該データベース内の当該データの詳細な所在を特定するファイル名情報（図１の１１２）と、上記データベースに登録したデータから予め定められた一方向性ハッシュ関数により計算した数値の認証子（図１の１１３）と、上記データベースに登録するデータに施す暗号処理に使用したワーク鍵情報（図１の１１４）とを格納することを特徴としている。

（ｂ）また、前記複数のデータベースの少なくとも一つには、当該データが格納されている保健医療カードごとに一意に付与されたＩＤ番号（図５の５０９、ＩＤｃ）と、当該データを暗号化するために使用したワーク鍵情報を該カードのマスタ鍵情報で暗号化した情報（$kK_M(K_W)$）、あるいは該マスタ鍵情報を暗号化して該ワーク鍵情報を生成するために使用した鍵暗号鍵情報（同Ｋｓ）と、該データベース内の当該データの詳細な所在を特定するファイル名情報（同ｆｉｌｅｎａｍｅ）とを記録しておくことも特徴としている。

【０００５】（ｃ）また、データ暗号化のための前記ワーク鍵情報の生成処理、データの暗号化処理、および認証子の生成・検証処理を上記保健医療カード内で行うことなく、全て端末通信装置で行う場合（図４（３）の場合）には、前記複数のデータベースの少なくとも一つには、当該データが格納されている保健医療カードごとに一意に付与されたＩＤ番号（ＩＤｃ）と、当該データを暗号化するために使用したワーク鍵情報を該カードのマスタ鍵情報で暗号化した情報（$K_M(K_W)$）と、該データベース内の当該データの詳細な所在を特定するファイル名情報（ｆｉｌｅｎａｍｅ）とを記録しておくことも特徴としている。

（ｄ）また、前記複数のデータベースの少なくとも一つ（図１の１０５）に登録されたデータ（図１の１０６）は、ある医療機関（図１の１０１）からの検索要求により、当該データが登録されているデータベースを通信網において特定するネットワークアドレス情報と、該データベース内の当該データの詳細な所在を特定するファイル名情報とに基づいて、該データベースから通信網（図１の１０３）を介し検索要求を行った医療機関の通信端末装置に転送（図６の６０５）されることも特徴としている。

（ｅ）また、前記検索要求を行った医療機関は、登録されたデータベースから転送してきた当該データを受け取ると（図６の６０５）、当該データに対して、データベース登録時に施され、暗号処理に用いられたワーク鍵情報を予めカードから得ておき、該ワーク鍵情報を基に復号処理を施す（図６の６０７）ことも特徴としている。

（ｆ）また、前記検索要求を行った医療機関は、上記復号処理（図６の６０７）を行ったデータに対して、予め定められた一方向性ハッシュ関数により認証子を計算し（図６の６０８）、該認証子と保健医療カード登録されている認証子とを比較し、比較の結果、同一と判定されたときには、上記復号処理を行ったデータは正しいものとして該医療機関のメモリに格納する（図６の６０８）ことも特徴としている。

【０００６】（ｇ）また、当該保健医療カードの媒体（図８のカード）は、上記データベース（図８のセンタ）と通信網を介して接続し、該データベースの一つに登録する各データごとに、該データベース内の当該データの詳細な所在を特定するファイル名情報（図８のｉｍａｇｅ０）を入手して、自媒体内に格納するが、その際に、該ファイル名情報を該保健医療カードと該データベースとが共有する鍵情報（Ｋｔ）により暗号化して（Ｋｔ（ｉｍａｇｅ０））通信する（図８の８０４）ことも特徴としている。

（ｈ）また、前記保健医療カードと当該データベースとが共有する鍵情報により暗号化して通信する際の暗号処理（図６の６０７）は、該保健医療カード（図７の７０４）の内部で行う（図４（１））ことも特徴としている。

（ｉ）また、前記複数の医療機関によって共有される少なくとも一つのデータベース（図８のセンタ）には、保健医療カードごとに一意に付与されたＩＤ番号（図８の８０７のＩＤｃ）とともに、当該データの詳細な所在を特定するファイル名情報（同８０７のｉｍａｇｅ０）を記録しておき、上記共有されるデータベースとは異なる各医療機関等のデータベース（図８の端末）には、該共有データベースの一つに登録されるデータに施す暗号処理に必要な少なくとも２つの鍵情報のうちの一つ（図８の８０６のＫｓ）とともに、上記保健医療カードごとに一意に付与されたＩＤ番号（同ＩＤｃ）を記録しておくことも特徴としている。

（ｊ）前記共有されるデータベースとは異なる各医療機関等のデータベース（図８の端末）には、該共有データベースの一つに登録されるデータに施す暗号処理に使用したワーク鍵情報（K_W）とともに、上記保健医療カードごとに一意に付与されたＩＤ番号（ＩＤｃ）を記録しておく（図８の８０６）ことも特徴としている。

【０００７】

【発明の実施の形態】本発明においては、データの盗聴を防止する対策としてデータ自身を暗号化する。データを暗号化する際には鍵が必要であるが、この鍵(以下、ワーク鍵と呼ぶ）を生成するためのマスタ鍵をカードごとにユニークに割り振る。そして、ＩＣカードのＩＤ番号とともに、各自に割り振られたマスタ鍵をＩＣカードに保存する。以上の作業は、地方自治体等の信頼できる第３者機関が行うことにより、住民にカードを発行する。信頼できる第３者機関では、カード発行に際してカード所有者とＩＣカードのＩＤ番号およびマスタ鍵を、第３者に知られぬように厳重に管理し保管しておく。次に、ある患者がある病院で診療を受け、その時に生じた

患者データをデータベースに登録する際には、データをワーク鍵で暗号化してデータベースに登録した後、そのデータを保存するデータベースのネットワーク上でのアドレスとデータベース上のデータを特定するための識別子であるファイル名をＩＣカードに保存する。次に、データ改竄を検知するために、所定のハッシュ関数を利用してデータの認証コードを作成しこれをＩＣカードに保存する。データのもともとの所有者である病院には、ＩＣカードのＩＤ番号とともにデータを暗号化するために使用したワーク鍵をカードのマスタ鍵で暗号化したもの、あるいはマスタ鍵を暗号化してワーク鍵を生成するのに使用した鍵暗号鍵の記録を保持しておく。

【０００８】以下、本発明の実施の形態を説明する。実施の形態としては、医療分野における保健医療カードと病院内のデータベースに保存されたカルテ情報を例にして説明する。図１は、本発明の第１の実施例を示す保健医療カード処理システム全体の構成図である。図１では、病院１０１と病院１０２の二つのエンティティ（実体）間での画像データの転送を想定している。病院１０１と病院１０２は、病院外部のネットワーク１０３に公開されたファイルサーバ１０４、１０５を備える。ファイルサーバ１０４、１０５には、病院で診察治療を受けた患者のカルテデータが登録されている。例えば、ファイルサーバ１０５には、ある患者のカルテ情報１０６が登録されていると想定する。また、患者は、保健医療カード１０７を所持している。この保健医療カード１０７の記憶領域には、保健医療カードの内容１０８に示すような患者基本情報１０９、画像データ部１１０、カード所有者ごとに定められたマスタ鍵１１５、およびカードＩＤ番号１１６の各項目が割り付けられている。すなわち、氏名、生年月日等の患者基本情報１０９に加えて、画像データ部１１０があるが、この画像データ部１１０には、実際に画像データのある病院の名称、その住所、画像が撮影された日付、撮影部位、撮影装置などの属性情報１１１、ネットワーク１０３につながれたファイルサーバを識別するアドレス情報１１２（これには、ファイル名も含まれる）、カルテ情報のメッセージダイジェスト（メッセージを凝縮したもの）である認証子１１３、およびワーク鍵１１４が含まれている。ここで、認証子１１３とは、コードデータとして配列された各値のうち、最初の値と次の値を演算し、その演算結果と次の値を演算し、その演算結果と次の値を演算し、順次繰り返し演算して、最終の演算結果を認証子１１３とするものである。

【０００９】図２は、図１における医療従事者端末の外観図である。図２に示すように、端末２０１にはカードリーダ装置２０２が接続されており、患者が所有する保健医療カードを挿入することにより、そのカードに情報を読み書きすることができる。また、医療従事者端末２０１から病院内部のネットワークを介して図１に示したファイルサーバ１０４，１０５にアクセスすることが可能である。なお、図２では、カードリーダ装置２０２は１台だけが接続されているが、通常は２台接続されていることによって、保健医療カードと後述の操作者カードとの間のやりとりの操作が容易となる。すなわち、カードとカードのやりとりを行う場合、１台のカードリーダ装置２０２だけのときには、交互にカードを出し入れする必要があるが、２台のカードリーダ装置２０２があれば、挿入したままでやりとりができる。最初に、保健医療カードに対するアクセス権について説明する。保健医療カードでは、個人の病歴等が記述されているため、カードに対して誰でもアクセスすることが可能であると、個人のプライバシーが守れなくなる。そこで、アクセスについてある程度制限を設ける必要性が生じる。通常、保健医療カードに対しては、医師、看護婦、検査技師等の職種によって扱うデータが特定される。従って、職種ごとにアクセス権を設定することができるので、本実施例でも、職種ごとにアクセスできるデータを異ならせる。また、保健医療カードに対してある種の操作を行う場合には、最初に操作者の認証とそのアクセス権を検証する必要がある。ここで、操作者の認証とは、該当する保健医療カードに関係するグループに属しているか否か（例えば、その患者の担当グループであるか否か）を識別することであり、保健医療カードのアクセス権とは、そのカードに登録されたデータにアクセスすることができる資格者か否か（例えば、医師であるか否か）を識別することである。操作者認証については種々の手法が存在するが、以下では操作者が保健医療カードとは異なる操作者カードを利用して行う方法について説明する。まず、保健医療カードには、職種毎に定められたマスタ鍵の全てを、カードアクセス者の全てに対して読み出すことも書き込むこともできないシークレットゾーンに埋め込まれている。所持者本人も、カードのどこに埋め込まれているかを知ることができない。例えば、医師についてはKD、看護婦についてはKN、放射線技師についてはKTのように、職種毎に異なるマスタ鍵が保健医療カードに埋め込まれている。次に、操作者カードについては、その操作者の職種に応じたマスタ鍵のみがカードのシークレットゾーンに埋め込まれる。例えば、医師であるならばマスタ鍵KDのみが医師の操作者カードに埋め込まれている。

【００１０】図３は、本発明の実施例における保健医療カードとオペレーションカード（操作カード）との間の操作者認証処理を示すシーケンスチャートである。保健医療カードと操作者カードとの間に次のやりとりを行うことにより、お互いが正当なアクセス者であることを認証する。なお、図２のカードリーダ装置２０２が２台接続されているものとする。以下で説明する方法は、３パス相手認証と呼ばれているよく知られた方法である。ここでは、操作者が医師であるものとして説明する。すな

わち、オペレーションカードのシークレットゾーンには、医師のアクセス権を検証するためのマスタ鍵ＫＭ２，操作者の認証を行うためのマスタ鍵ＫＤが埋め込まれているのに対して、保健医療カードのシークレットゾーンには、職種毎のマスタ鍵ＫＤ，ＫＮ，ＫＴとアクセス権検証のためのマスタ鍵ＫＭ１が埋め込まれている。なお、ここには示されていないが、保健医療カードのＩＤであるＩＤｃ、操作者カードのＩＤであるＩＤｏが、それぞれのカードに埋め込まれている。

①「操作者認証処理」

［ステップ３０１］保健医療カードは乱数ＲＣを生成し、これを操作者カードに送信する。

［ステップ３０２］操作者カードは乱数ＲＯを生成し、ステップ３０１で受け取ったＲＣと、操作者カードのＩＤであるＩＤｏを医師のマスタ鍵KDで暗号化し、医師を表すフラグＤｏｃとともに保健医療カードに送信する。なお、医師を表すフラグＤｏｃは、保健医療カード側に対して確かに医師であることを知らせるためのフラグである。

【００１１】［ステップ３０３］保健医療カードはステップ３０２で送られてきた電文から、医師を表すフラグＤｏｃによりマスタ鍵KDを選択し、暗号化された部分を復号化してＲＣ、ＲＯ、ＩＤｏを得る。復号化されたＲＣを先に生成したＲＣと比較して、ステップ３０２で電文を送信してきた相手が医師であることを認証する。

［ステップ３０４］ステップ３０３で得られたＲＣ、ＲＯと保健医療カードのＩＤであるＩＤｃ、そして保健医療カード内で生成したテンポラリ鍵Ｋｔをマスタ鍵KDで暗号化し、操作者カードに送信する。なお、テンポラリ鍵Ｋｔは、同じ鍵を用いてやりとりする場合に、セッションごとに内容の異なる鍵Ｋｔを送信することにより、安全性を保持する。

［ステップ３０５］操作者カードはステップ３０４で送られてきた電文を、マスタ鍵KDで復号化しＲＣ、ＲＯ、ＩＤｃ、Ｋｔを得る。復号化されたＲＯを先に発生したＲＯと比較し、ステップ３０３で電文を送信してきた相手が正当な保健医療カードであることを認証する。この手続きにより、保健医療カード側は操作者が医師であることを認証することができる。

【００１２】次に、病院１０２において、ファイルサーバ１０５に画像データ１０６を登録する処理について説明する。図４は、医療従事者端末側と保健医療カード側における登録処理のモジュール構成図であって、３通りのパタンを図示したものである。パタン（１）は暗号化のためのワーク鍵の生成４０３や暗号化処理４０２、ならびに認証子の生成検証４０４をすべてカード側で行うものである。このパタンでは、暗号化処理４０２をカードで行うことにより暗号鍵が一時的でもカードの外に漏れることがないので安全性が極めて高い。パタン（２）では、パタン（１）の暗号化処理４０２のみを医療従事者端末側に移したものである。画像のような大容量データの暗号化処理には、大きな計算処理能力が必要とされる。カード側のマイクロプロセッサは、通常その計算処理能力に限界があるため、大きな計算処理能力が必要とされる処理を医療従事者端末側に移すことにより、カード側の負担を軽くできる。しかし、カードで生成したワーク鍵が医療従事者端末側に一時的に漏れるため、このワーク鍵を記録しておき、その後に不正を行うことが可能であり、その結果、安全性が低くなる。パタン（３）では、暗号化のためのワーク鍵の生成４０３や暗号化処理４０２、ならびに認証子の生成検証４０４をすべて医療従事者端末側で行うものである。このタイプでは、ワーク鍵の生成から暗号処理まで全て端末側で行うため安全性は低い。しかし、運用面での効率を高めることができる。パタン（１）（２）のタイプでは、患者の保健医療カードがない限り、暗号化のワーク鍵が生成できないので、暗号化処理ができない。従って、複数患者のデータを前もって暗号化しておくことができないため、データ登録処理のスループットも上げることができない。一方、パタン（３）のタイプでは、暗号化処理に必要なワーク鍵は端末側で生成しており、保健医療カードはこのワーク鍵を登録するだけであるため、端末側で複数患者データを一括処理しておくことが可能である。

【００１３】図５は、図４における登録処理のためのデータのフローを示した図である。画像データを図１のファイルサーバ１０５に登録するために、まず、患者の所有する保健医療カード１０７を、図２の医療従事者の端末２０１に接続されたカードリーダ２０２にセットする。

②「登録処理」

［ステップ５０１］前述した「操作者認証処理」を図４のカードアクセスマネージャ４０６を介し、アクセス権チェックモジュール４０１で行うことにより操作者を認証する。なお、アクセス権チェックモジュール４０１は、操作者認証処理およびアクセス権チェックの両方を行う。以下のステップ５０２以降は、操作者が医師、看護婦、放射線技師でないと進めない。

［ステップ５０２］登録処理を行うことを図４のカードアクセスマネージャ４０６が認識すると、記憶領域４０５中の画像データ部（図１の１１０）の領域内に、新規登録の画像のための領域（斜線部分）を確保する。

［ステップ５０３］図４のカードにおけるワーク鍵生成モジュール４０３は鍵暗号鍵Ｋｓを生成し、カードに記憶されたマスタ鍵（図１の１１５）により暗号化して、ワーク鍵を生成する。

［ステップ５０４］ステップ５０３で生成したワーク鍵を、ステップ５０２で確保した図４の記憶領域４０５のワーク鍵領域（図１の１１４）に登録する。

［ステップ５０５］図４のカードアクセスマネージャ４０６は、図２の画像データを端末２０１のディスク装置

（図５の右側部分）から読み込みマネージャ内のバッファに蓄積する。

［ステップ５０６］図４のカードアクセスマネージャ４０６は、ステップ５０５で読み込んだ画像データをカード側の認証子生成検証モジュール４０４に送出する。図４の認証子生成検証モジュール４０４では、画像データからあらかじめ定めたハッシュ関数により認証子を計算し、ステップ５０２で確保した図４の記憶領域４０５の認証子領域（図１の１１３）に登録する。

【００１４】［ステップ５０７］図４のカードアクセスマネージャ４０６は、ステップ５０５で読み込んだ画像データをカード側の暗号処理モジュール４０２に送出する。図４の暗号処理モジュール４０２では、ステップ５０３で生成したワーク鍵により画像データを暗号化する。

［ステップ５０８］ステップ５０７で暗号化された画像は、図４のカードからカードアクセスマネージャ４０６を介して公開ファイルサーバ（公開サーバストレージ）（図１の１０５）に登録される。この時、図４のカードアクセスマネージャ４０６は、登録する画像のファイル名image0を自動的に付与し、この名前で公開ファイルサーバ（図１の１０５）に登録するとともに、ファイルサーバ（図１の１０５）のアドレス情報とファイル名image0をステップ５０２で確保した図４の記憶領域４０５のアドレス部（図１の１１２）に登録する。

［ステップ５０９］図２の端末２０１のディスク装置に、保健医療カード（図１の１０７）のＩＤであるＩＤｃとステップ５０３で生成した鍵暗号鍵Ｋｓとステップ５０５で付与されたファイル名image0の組［ＩＤｃ，Ｋｓ，image0］を保存する。このようにして、もし図１のファイルサーバ１０５に登録する画像データが複数存在する場合には、ステップ５０２からステップ５０９までの処理を登録する画像データの個数分だけ繰り返す。上記実施例を、図４（３）のタイプのカードシステムで実装した場合には、ステップ５０９における鍵暗号鍵Ｋｓのかわりに、画像を暗号化する時に使った、ワーク鍵をカードのマスタ鍵で暗号化したもの（つまり、$K_M(K_W) = K_M(K_M(K_M))$）を保存する必要がある。

【００１５】次に、上記の登録処理の効果について述べる。図１において、少なくとも病院１０２のシステム管理者は、ファイルサーバ１０５上のファイルを自由に読み書きすることができると考えるのが普通である。従って、病院がデータを都合のいいように書き換えてしまうことが考えられるので、データ改竄を何らかの方法で検知する必要がある。従来より、データのメッセージダイジェストをハッシュ関数で計算し、それをワーク鍵で暗号化してファイルに添付しておく方法が良く取られる。これにより、ワーク鍵を知らない限り、改竄の事実を隠すようにファイルに細工をすることは不可能である。しかしながら、図４（３）のように殆んどの処理を端末側で行うカードシステムを採用すると、ワーク鍵が病院側に知れてしまうので、ファイルに認証子を付加する方法は有効ではない。すなわち、ファイルに認証子を付加するだけでは、ファイルサーバ１０５に登録した画像を改竄して、所定のハッシュ関数で計算したメッセージダイジェストを上記ワーク鍵で暗号化して改竄画像に付加し、それをファイルサーバ１０５の登録画像と入れ替えればよいからである。一方、暗号処理の高速化を図ったり、画像登録処理のスループットを上げるために、図４（３）のような構成を採用することが必要となる。そこで、本実施例のようにファイルサーバ１０５に登録する画像の認証子をカード側に登録しておけば、図４（３）のモデルを採用しても、認証子を改竄することは事実上不可能であるため、病院側にワーク鍵が知れても全く問題はない。

【００１６】図５のステップ５０５では、画像を暗号化して図１のファイルサーバ１０５に登録するが、このように暗号化する理由は、ファイルサーバ１０５がネットワーク１０３に公開されていることから、病院外部の第３者にデータを盗聴されないようにするためである。次に、患者が自分の保健医療カード１０７を紛失してしまった時のことを考える。患者は、カードを紛失したことをカードを発行した機関に届け、再びカードを発行してくれるよう要請する。ここで、カードを発行した第３者機関は、初めにカードを発行した際のマスタ鍵を、カードのＩＤとともに厳重に管理している。従って、カード再発行の要請に対して、カードのＩＤとマスタ鍵は復元することができる。患者は再発行された保健医療カードを持参して病院１０２に行き、保健医療カードのＩＤであるＩＤｃにもとづき、図５のステップ５０９で保存した［ＩＤｃ，Ｋｓ，image0］から、ファイル名image0に関する画像情報について、その認証子を除いたカード内情報は復元することが可能である。この場合、第３者機関のカード再発行処理は、厳しい運用規則の下で行われることが必要である。何故ならば、第３者の他人にカードを発行してしまうと、その第３者は上記データ復元処理で他人のデータを収集することが可能になってしまうためである。従って、カードの再発行処理は、本人自からが再発行を要請していることを十分確認した上で行われることが必要である。

【００１７】いま仮に、医療従事者以外の第３者が、ある患者になりすましてカードを偽造し、上記データ復元処理によりデータを不正に入手することを試みたとする。この場合にも、データの機密性は確保できることを説明する。まず、カードＩＤ番号はネットワーク上に漏れることがあるので、何らかの方法で第３者が入手することは可能である。従って、このＩＤを偽造カードに埋め込み、上記データ復元処理のプロセスを踏めば、データの所在であるファイル名と鍵暗号鍵であるＫｓが入手できる。しかし、この不正入手したファイル名からデー

タを盗んだとしても、データの内容を見るためには、鍵暗号鍵Ｋｓと不正入手したＩＤに対応するマスタ鍵からワーク鍵を生成する必要がある。しかし、マスタ鍵はネットワークに漏れないこと、また、第３者機関が厳重に管理していることから、医療関係者以外が不正に入手することは事実上不可能である。従って、医療従事者以外の第３者が、データの内容を見ることは事実上不可能である。図４（３）のタイプのカードシステムで実装した場合にも、上述と同様な理由で、ワーク鍵をマスタ鍵で暗号化したものとファイル名を不正に入手できたとしても、ワーク鍵本体を知るためにマスタ鍵が必要である。従って、データの内容を見ることは事実上不可能である。なお、図４（１）のように暗号化処理モジュール４０２をカード内部に実装している場合には、図５のステップ５０９で端末２０１のディスク装置に、保健医療カード１０７のＩＤであるＩＤｃと、ステップ５０３で生成した鍵暗号鍵Ｋｓと、ステップ５０５で付与されたファイル名image0、ステップ５０６で計算した認証子をステップ５０３で生成したワーク鍵で暗号化したKw(code)の組［ＩＤｃ，Ｋｓ，image0,Kw(code)］を保存してもよい。このときは、カード紛失時に認証子も復元することができる。なお、codeは、認証子のコードを示す。

【００１８】次に、図１の病院１０１に来院した患者に対して、他病院での診察情報を検索する時の検索処理について説明する。図６は、本発明における検索処理についてのフローを示した説明図である。ここでは、図１の病院１０２にあるネットワーク１０３につながれたファイルサーバ１０５に保存されたファイルimage0を検索し、病院１０１のファイルサーバ１０４にダウンロードすることを想定して説明する。検索処理に対しても図４（１），（２），（３）のそれぞれのタイプが考えられるが、登録処理と同じようにそれぞれのタイプについて安全性の面では違いがあるものの、処理自体は基本的に変わらないので、ここでは図４（１）のタイプについて説明する。まず、患者の所有する保健医療カード１０７を、医療従事者の端末２０１に接続されたカードリーダ２０２にセットする。

③「検索処理」

［ステップ６０１］前述した「操作者認証処理」を、図４のカードアクセスマネージャ４０６を介してアクセス権チェックモジュール４０１で行うことにより、操作者を認証する。次のステップ６０２以降は、操作者が医師、放射線技師でないと進めない。

［ステップ６０２］図１の保健医療カード１０７の画像データ部１１０に含まれる属性情報１１１が記憶された領域のデータを、図２のカードリーダ２０２を介して読み込み、医療従事者端末２０１の画面に表示する。

【００１９】［ステップ６０３］表示された属性情報から、たとえば日付、撮影部位などの情報をもとに端末操作者が検索する画像を画面から選択する。

［ステップ６０４］ステップ６０３で選択された画像に対して、図４のカードアクセスマネージャ４０６は画像データ部（図１の１１０）に含まれるアドレス情報１１２を保健医療カード１０７から読み込む。そして、カードアクセスマネージャ４０６は、読み込んだアドレス情報をネットワークマネージャ４０７に送る。ここでは、図１の病院１０２のファイルサーバ１０５のアドレスおよびファイルimage0を選んだものとして、以下の説明を進める。

［ステップ６０５］ステップ６０３で得たアドレス情報をもとに、図４のネットワークマネージャ４０７はネットワーク１０３上にあるファイルサーバ１０５にアクセスを試み、該当ファイルを図１の病院１０１にあるファイルサーバ１０４にダウンロードする。この場合、病院１０２にあるファイルサーバ１０５のファイルimage0が、ネットワーク１０３を通じて病院１０１にあるファイルサーバ１０４にダウンロードされることになる。

［ステップ６０６］図４のネットワークマネージャ４０７は、ステップ６０５でファイルサーバ１０４にダウンロードした画像データを図２の医療従事者端末２０１に取り込んだ後、カードアクセスマネージャ４０６に送り、カードアクセスマネージャ４０６は画像データをカード内部の暗号処理モジュール４０２に送り込む。

【００２０】［ステップ６０７］図４の暗号処理モジュール４０２では、ステップ６０６で取り込んだ画像データを、図１の画像データ部１１０に含まれる当該画像データのワーク鍵領域１１４に登録されたワーク鍵をもとに復号処理を行う。そして、復号された画像を、認証子生成検証モジュール４０４に送り込む。

［ステップ６０８］図４の認証子生成検証モジュール４０４では、上記復号処理で復号された画像データに対して、あらかじめ定められたハッシュ関数により認証子を計算する。次に、この認証子と図１の画像データ部１１０に含まれる当該画像データの認証子領域１１３に登録されたものとを比較する。比較した結果、同じと判定されれば復号した画像データを端末に接続されたローカルなディスクに吐き出す。本検索処理の効果について以下説明する。まず、本検索処理により、ネットワーク上のファイルサーバにあるデータを、カードに記録されたアドレス情報からダウンロードすることができるので、あたかもカード内に記録されたデータのように入手することが可能になる。また、ステップ６０５では、図１のネットワーク１０３を通じてデータをダウンロードするが、データは登録処理によってあらかじめ暗号化されているので盗聴の心配はない。また、ネットワーク上での改竄も、ステップ６０８における認証子の検証により、改竄が検知できる。従って、オフライン型の保健医療カードと同様の安全性を確保することができる。

【００２１】前実施例では、患者データをその発生源で分散管理する方式で説明した。次の実施例では、必要に

応じて地域毎に設置されたサーバにデータを保管できる方式について説明する。図７は、本発明の他の実施例を示すカード処理システムの全体構成図であり、図８は、図７におけるデータ登録処理のシーケンスチャートである。図７に示すように、地域医療情報センタ７０１にはファイルサーバ７０２が設けられており、このサーバ７０２に対して地域全体の医療機関からアクセスされることによって、患者データの共有化を図ることができる。このファイルサーバ７０２は、各病院と独立であるが、地域自治体の管理下におかれているため、内部の人間に蓄積されたデータを盗聴されたり改竄されたりする可能性があると仮定する。本実施例では、病院７０３がある患者の画像データを地域医療情報センタ７０１のファイルサーバ７０２に登録する処理について説明する。本実施例では、カードシステムとしては図４（１）のタイプを採用しなければならない。以下、図８に従ってデータ登録処理の手順を説明する。

④「登録処理」

［ステップ８０１］図３で説明した「操作者認証処理」を、図４のカードアクセスマネージャ４０６を介してアクセス権チェックモジュール４０１で行うことにより、病院７０３側にある患者の保健医療カード７０４と地域医療情報センタ７０１のファイルサーバ７０２との認証処理を行う。すなわち、図７の医療従事者端末におけるカードアクセスマネージャ４０６が、カードリーダに挿入されたカード７０４に対して操作者の認証処理を行う。このとき、端末側より医療情報センタおよびカードにテンポラリ鍵Ｋｔを送出する。認証処理に失敗した場合には、以下のステップには進めない。

［ステップ８０２］図５に示した「登録処理」のステップ５０２からステップ５０７を実行する。これらの処理ステップにより、暗号処理、認証子生成処理が行われて、ワーク鍵Ｋｗ，認証子ｃｏｄｅ、データｄａｔａがカード側へ、またデータをワーク鍵で暗号化したＫｗ（ｄａｔａ）がセンタ側へ、それぞれ送出される。

［ステップ８０３］図４の端末におけるカードアクセスマネージャ４０６は、地域医療情報センタ７０１のファイルサーバ７０２にファイル名を要求する。

【００２２】［ステップ８０４］センタ７０１のファイルサーバ７０２は、この要求に対して「操作者認証処理」で得られたテンポラリ鍵Ｋｔを暗号鍵としてファイル名image0を暗号化し、Ｋｔ（image0）を図４のカードアクセスマネージャ４０６を経由して端末７０６の保健医療カード７０４に送る。暗号化されたファイル名Ｋｔ（image0）を受信した保健医療カード７０４は、「操作者認証処理」でＫｔを知っているので、暗号化されたファイル名Ｋｔ（image0）を復号して元のファイル名image0を知る。そして、ファイルサーバ７０２のアドレス情報と得られたファイル名image0を、ステップ５０２で確保した図４の記憶領域４０５のアドレス部（図１の１１２）に登録する。

［ステップ８０５］図５のステップ５０６で生成した認証子をステップ５０３で生成したワーク鍵Ｋwで暗号化し、さらにテンポラリ鍵Ｋｔにより暗号化Ｋｔ（Ｋw（ｃｏｄｅ））して、カード７０４からカードアクセスマネージャ４０６に送る。そして、Ｋｔ（Ｋw（ｃｏｄｅ））と暗号化画像をネットワークマネージャ４０７を介してセンタ７０１のファイルサーバ７０２に送信する。ファイルサーバ７０２に送られてきた暗号化画像は、上記ファイルサーバ７０２で発行されたファイル名image0でファイルサーバ７０２に登録される。同時に、暗号化された認証子Ｋｗ（ｃｏｄｅ），暗号化画像Ｋｗ（ｄａｔａ）もファイルに蓄積される。

［ステップ８０６］保健医療カード７０４は、鍵暗号鍵Ｋｓを病院７０３の保護されたディスク装置７０６に保健医療カードのＩＤであるＩＤcとともに保存しておく。

［ステップ８０７］ファイルサーバ７０２は、図３に示す「操作者認証処理」のステップ３０５で得られた保健医療カード７０４のＩＤであるＩＤcとともに、ステップ８０３で得たファイル名image0、ステップ８０５で得たＫｔ（Ｋw（ｃｏｄｅ））をＫｔで復号化したＫw（ｃｏｄｅ）を保存しておく。

【００２３】次に、図７の実施例の効果を説明する。本実施例を採用することにより、患者データは地域保健医療情報センタ７０１で一括管理されているため、データを登録した病院、あるいはその病院の医師が証拠隠滅のためにデータを消去してしまうことが不可能となる。また、本実施例のような集中管理のメリットとしては、各病院のファイルサーバの記憶容量を削減することができる等が挙げられる。一方、地域保健医療情報センタ７０１には、地域住民の患者データが集中するので、プライバシー保護の観点からあまり好ましくない。また、上記の前提で述べたように、地域医療情報センタの内部の人間がファイルサーバに蓄積されたデータを盗聴したり改竄したりする可能性もある。しかし、地域保健医療情報センタ７０１のファイルサーバ７０２のデータは、患者の保健医療カード７０４に保存されたワーク鍵で暗号化されているため、ワーク鍵を入手しない限りそのデータの内容を見ることはできない。また、改竄したとしても、保健医療カードの認証子を検証することにより、その改竄を検知することができる。

【００２４】ここでは、患者が自分の保健医療カードを紛失した場合を想定し、その対策方法を説明する。この場合には、図７の地域医療情報センタ７０１と病院７０３、そして患者が合意することによって、病院７０３における患者のデータを復元することができる。患者は、カードを紛失したことをカードを発行した機関に届け、カードの再発行を要請する。前実施例と同じように、カードを発行した機関は、初めにカードを発行した際のマ

スタ鍵を、カードのＩＤとともに厳重に管理している。従って、カード再発行の要請に対しても、カードのＩＤとマスタ鍵は復元することができる。図８のステップ８０７で、図７のファイルサーバ７０２は、保健医療カードのＩＤであるＩＤcとともにファイルサーバ７０２に登録するデータのファイル名（image0）とワーク鍵Ｋｗで暗号化された認証子（Ｋｗ(code)）を保存しておくので、このＩＤをもとにしてファイル名とワーク鍵Ｋｗで暗号化された認証子をファイルサーバ７０２から収集してくることが可能である。また、ステップ８０６で、図７のファイルサーバ７０５は、保健医療カードのＩＤであるＩＤcとともに鍵暗号鍵Ｋｓを保存しておくので、このＩＤをもとにして鍵暗号鍵Ｋｓをファイルサーバ７０５から収集してくることが可能である。従って、新しく発行された保健医療カードのマスタ鍵Msとファイルサーバ７０５から集めた鍵暗号鍵Ｋｓにより、全てのワーク鍵を復元することができるので、暗号化された認証子（Ｋｗ(code)）も復元することが可能になる。

【００２５】前の実施例と同じように、医療関係者を含む第３者がカードを偽造し、本人になりすましてデータを不正入手したり、その内容を盗み見ることは事実上不可能である。何故ならば、本実施例では、カードシステムとして図４（１）を採用しているので、医療関係者でさえもマスタ鍵を知ることはできない。そして、マスタ鍵がない限りワーク鍵を知ることもできないことから、地域医療情報センタ７０１に登録されたデータを復号することができないためである。なお、ステップ８０６では、病院７０３の保護されたディスク装置７０６に、ワーク鍵を生成するのに使用した鍵暗号鍵Ｋｓを保存しているが、これとは別の場所にカードのＩＤとともにワーク鍵を保存しておくことを考える。この場合、病院側がワーク鍵を知っていてもデータの秘密が漏れる必配のないことは、前述の通りである。すなわち、前の実施例の登録処理の効果において説明したように、認証子をカードに登録するため、データが改竄された場合には、認証子を用いて検証すれば確実にこれを検知できるためである。ただし、上記カード復元のプロセスにおいて、このワーク鍵を絶対にカード紛失者（カード偽造者になり得る者）に知らせてはならないことに注意すべきである。上記のように別の場所にワーク鍵を保存する形態をとるメリットは、ある緊急事態、例えば患者がカードを所有していないときに事故に遭遇した場合などに、患者の過去の医療情報が知りたいとき、患者の同意を得られればカードがなくとも、地域医療情報センタ７０１は患者のＩＤとともに緊急を知らされる情報を含んだ電文を全国に同報通信しワーク鍵を病院から入手して患者情報を復号し、他の病院に緊急にこのデータを送信することが可能になることである。

【００２６】前述のように、オフライン型保健医療カードでは、カードに記録されたデータを見たり、データにある種の操作を加えるためには、患者が保健医療カードを医師などに渡してデータの権利を委譲することが必須事項となる。従って、カードに対するアクセス管理がしっかりしていれば、安全性はかなり強固であると言える。これに対して、保健医療カードシステムをオンラインデータベースと連携させると、患者データの一部がネットワーク上のデータベースに蓄積されることになるため、どうしても盗聴、改竄などの脅威にさらされることになる。また、オンラインデータベースと連携させると、通常は正当なシステム管理者やユーザが何らかの原因により突然に不正者になった場合には、データを不正に操作することが可能になる。本発明においては、オンラインデータベースと連携させることにより生じる上述のような特有な問題を解消することができるので、従来のオフライン型保健医療カードと同じ安全性を、オンラインデータベースと連携した保健医療カードシステムでも実現可能となる。そして、オフライン型保健医療カードでは実現が難しい、カードを紛失したときにその内容を復元する方法を実現することができる。

【００２７】

【発明の効果】以上説明したように、本発明によれば、従来のオフライン型保健医療カードと同じ安全性を、オンラインデータベースと連携した保健医療カードシステムでも実現することができるとともに、カードを紛失したときにも、オンラインデータベースから安全にカードの内容を復元することができる。

【図面の簡単な説明】

【図１】本発明の一実施例を示す保健医療カード処理システム構成およびカードの内容を示す図である。

【図２】図１における医療従事者端末とカードリーダの概観図である。

【図３】本発明の一実施例を示す保健医療カードとオペレーションカード間の認証処理のシーケンスチャートである。

【図４】本発明の一実施例を示すカード内部と医療従事者端末のモジュール構成図である。

【図５】本発明の一実施例を示すデータ登録処理のフローを説明する図である。

【図６】本発明の他の実施例を示すデータ検索処理のフローを説明する図である。

【図７】本発明の他の実施例を示す保健医療カードシステムの構成図である。

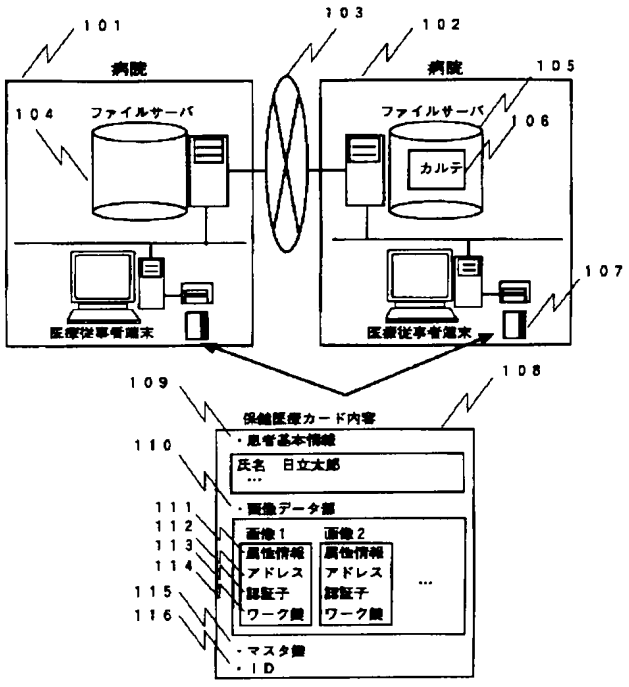
【図８】図７におけるデータ登録処理のシーケンスチャートである。

【符号の説明】

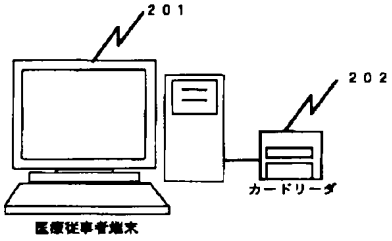
１０１：病院、１０２：病院、１０３：ネットワーク、１０４，１０５：ファイルサーバ、１０６：電子カルテ、１０７：保健医療カード、１０８：保健医療カードの内容、１０９：患者基本情報、１１０：画像データ部、１１１：属性情報、１１２：アドレス、１１３：認

証子、１１４：ワーク鍵、１１５：マスタ鍵、１１６：ＩＤ、２０１：医療従事者端末、２０２：カードリーダ、４０１：アクセス権チェックモジュール、４０２：暗号処理モジュール、４０３：ワーク鍵生成モジュール、４０４：認証子生成検証モジュール、４０５：記憶領域、４０６：カードアクセスマネージャ、４０７：ネットワークマネージャ、５０１：相手認証処理、５０７：暗号処理、
５０２：カード内記憶領域の確保処理、５０３：ワーク鍵生成処理、５０４：ワーク鍵登録処理、５０５：データのロード、５０９：ログ記録処理、
５０６：認証子生成処理、６０１：相手認証処理、６０３：データ選択処理、５０８：公開サーバへのデータ登録処理とカードへのファイル名の登録処理、６０２：カード内記憶内容の表示、８０６：病院におけるログ記録処理、６０４：データアドレスをネットワークマネジャーに通知、６０５：データのダウンロード、６０７：暗号処理、７０２：ファイルサーバ、
７０１：地域医療情報センタ、７０３：病院、７０４：保健医療カード、６０６：カード内部の暗号処理モジュールにダウンロードしたデータ送信、８０７：地域医療情報センタにおけるログ記録処理、７０５：ファイルサーバ、
６０８：認証子検証処理およびローカルディスク上へのデータの送信、７０６：保護されたディスク装置、８０１：相手認証処理、８０２：暗号処理、認証子生成処理、８０３：ファイル名の要求、８０４：ファイル名の付与とカードへの送信、８０５：画像および鍵暗号鍵により暗号化された認証子の地域医療情報センターファイルサーバへの送信。

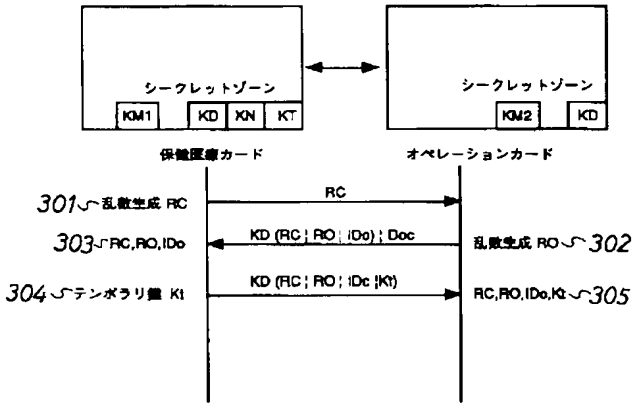
【図１】



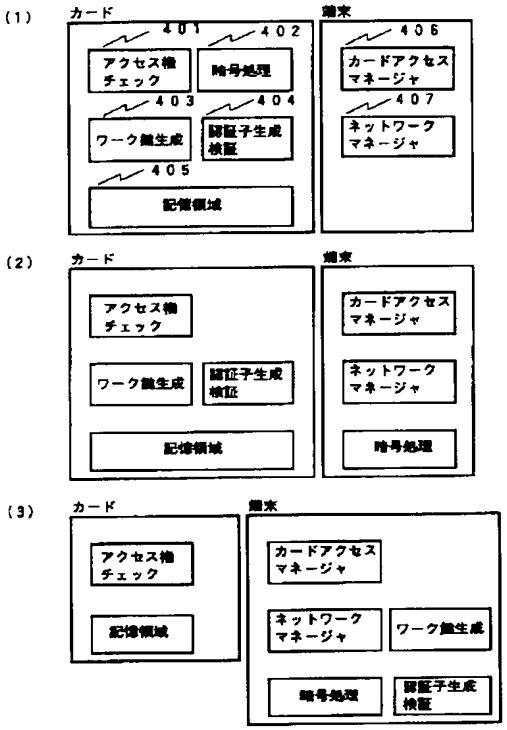
【図２】



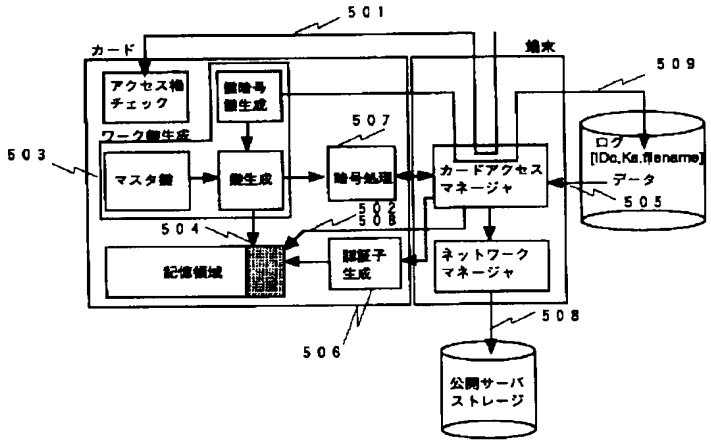
【図３】



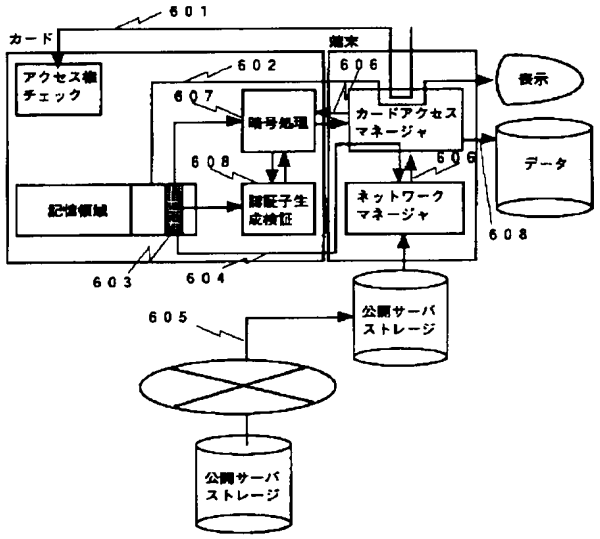
【図４】


(1)
カード
端末
401
402
406
アクセス権チェック
暗号処理
カードアクセスマネージャ
403
404
407
ワーク鍵生成
認証子生成検証
ネットワークマネージャ
405
記憶領域
(2)
カード
端末
アクセス権チェック
カードアクセスマネージャ
ワーク鍵生成
認証子生成検証
ネットワークマネージャ
記憶領域
暗号処理
(3)
カード
端末
アクセス権チェック
カードアクセスマネージャ
記憶領域
ネットワークマネージャ
ワーク鍵生成
暗号処理
認証子生成検証

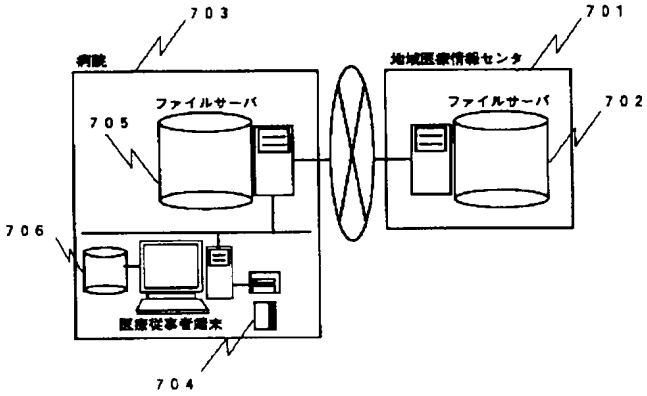
【図５】


501
カード
端末
509
アクセス権チェック
暗号鍵生成
ワーク鍵生成
507
503
マスタ鍵
鍵生成
暗号処理
カードアクセスマネージャ
ログ [IDc,Ks,filename]
データ
505
502
504
508
記憶領域
認証子生成
ネットワークマネージャ
506
508
公開サーバストレージ

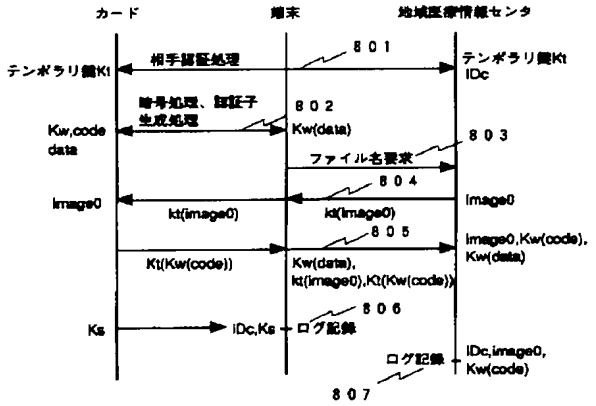
【図６】


601
カード
端末
アクセス権チェック
602
606
表示
607
暗号処理
カードアクセスマネージャ
608
509
データ
記憶領域
認証子生成検証
ネットワークマネージャ
603
604
608
605
公開サーバストレージ
公開サーバストレージ

【図７】


703
701
病院
地域医療情報センタ
ファイルサーバ
ファイルサーバ
705
702
706
医療従事者端末
704

【図８】


カード
端末
地域医療情報センタ
801
相手認証処理
テンポラリ鍵Kt
テンポラリ鍵Kt
IDc
暗号処理、認証子生成処理
802
Kw,code data
Kw(data)
803
ファイル名要求
804
Image0
kt(Image0)
kt(Image0)
Image0
805
Image0,Kw(code),Kw(data)
Kt(Kw(code))
Kw(data),kt(Image0),Kt(Kw(code))
806
Ks
IDc,Ks
ログ記録
ログ記録
IDc,Image0,Kw(code)
807